Walsh Memorial CE (VC) Infant School

ONLINE SAFETY POLICY

Autumn 2023
Review Autumn 2024

This policy is part of the school's safeguarding responsibilities. It relates to other policies including those for behaviour, safeguarding and data handling.

Our Online Safety Manager works alongside the Designated Safeguarding Lead (DSL) as the roles overlap. The Online Safety Manager is Mrs Timmins.

- Our online safety policy has been written by the school community, building on best practice and government guidance.
- The online safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, phones, tablets and hand held games consoles used on the school sites

Teaching and learning

Why Internet and digital communications are important

- Internet use is a part of the statutory curriculum and a necessary tool for staff and children
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Children will be shown how to publish and present information appropriately to a wider audience.
- Children will be taught online safety in accordance with the Teach Computing and Project Evolve schemes of work for the Infant school and the Switched-on Computing and Gooseberry planet schemes for the Junior school and reinforced regularly. It aims to bridge the gap between school IT systems and the more open systems outside of school.
- The school will have an age-appropriate filtering system
- The school will ensure that its networks have virus and anti-spam protection
- Access to the internet is password protected
- Online safety will be embedded in all areas of the curriculum
- Children will be taught the earliest skills of building resilience to radicalization by providing a safe environment for discussing controversial issues. The school will ensure that children are safe from terrorist and extremist material
- Children will be taught about the importance of safe use of passwords

Managing Internet Access

Information system security

- School ICT systems security will be reviewed annually
- Virus protection will be updated regularly

- Children will only have access to wireless devices owned by the school and staff and children are not permitted to bring their own devices to school (this includes smart watches).

E-mail

- All children will be taught that we can send and open polite and friendly e-mails to people we know
- All digital communications with parents and pupils should be on a professional level and on a school system

Published content and the school web site

- Staff or children's personal information will not be published – children will be identified by first name and initial of surname only, staff by title and surname.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- The school web site has links to NSPCC online safety, internet matters.org and child protection and online protection to support parents knowledge of e safety and online gaming support.

Social networking

- Social networking sites will only be used if it enhances the life of the school
- Children and parents will be advised that the use of social media outside school brings a range of dangers for primary aged pupils

Publishing children's images and work

- Written permission from parents or carers will be obtained before photographs of children are published on the school website
- The school will ensure that the use of photographs on the school website will not allow children to be identified by surname
- The online-safety policy will be shared with parents on induction and will be available on the website

Managing filtering

- The school will work in partnership with an external IT support provider to ensure systems to protect children are in place.
- If staff or children come across unsuitable on-line materials, the site must be reported to a DSL who will inform the external IT support provider. It will then be blocked.
- The DSL team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school has a SENSO account that monitors key words, this immediately alerts the DSL and can identify the computer that was used.
- Serious breaches of this policy by a member of staff will be reported to Surrey County Council LADO
- Parents will be informed of any incidents of inappropriate online safety behaviour that takes place in school. Incidents of inappropriate behaviour that is outside of the school will only be investigated if it is linked to a member of the school community.
- The school regularly reviews the www.testfiltering.com at least annually
- The school will complete the https://360safe.org.uk/ which will provide a comprehensive review and an entire approach to online learning.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- I Pads and associated cameras will be used during lessons or formal school time for taking photographs, as part of an educational activity.
- Sony Play station, Microsoft Xbox etc will not be used in school unless a risk assessment has been carried out.
- Staff will use a school phone where contact with children or parents is required unless on a school trip or otherwise unavailable in which case dial 141 before the number is dialled to protect identity.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- All staff must read and sign the 'Acceptable Use Agreement' before using any school ICT resource
- Any person not directly employed by the school will be asked to sign the 'Acceptable Use Agreement' before using any school ICT resource
- When pupils have free access to search the internet, staff will be vigilant in monitoring the content of the site visited.
- Parents will be asked to sign and return an internet access consent form which is part of the home-school agreement

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Introducing the Online safety policy to children

- Appropriate elements of the Online-safety policy will be shared with pupils
- Pupils will gain awareness of Online-safety and cyber bullying through the Online-safety Scheme of Work made from a combination of Teach Computing and Project Evolve for the Infant school and a combination of Switched-on Computing and Gooseberry planet for the Junior school which will be taught throughout the school as a discrete topic at the beginning of each unit of work in Computing and woven throughout the curriculum when appropriate

Staff and the E-safety policy

- Online safety training is completed by all staff as part of the safeguarding training delivered at the start of every academic year
- Additional training is delivered at staff meetings as and when required

- Regular weekly safeguarding updates will include regular online safety questions
- When asked to sign the Acceptable Use Agreement, all staff will be aware of and have access to the school's online safety policy
- Staff should be aware that Internet access can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Parents' and carers' attention will be drawn to the school's online safety policy in newsletters and on the school web site
- Parents and carers will from time to time be provided with additional information on online safety
- Online gaming safety advice are shared with parents and are shared on the online safety page on the school website

Ensuring Compliance

- Any concerns should be reported to a DSL
- Concerns about breaches of the online safety policy or Acceptable Use Agreement should be referred to the Headteacher
- Concerns of a child protection nature must be dealt with in accordance with school safeguarding procedures
- Children and parents will be informed of consequences for children misusing the Internet.
- The use of mobile phones during the teaching day is not permitted by staff, visitors or parent volunteers in school.

Link to other policies:
Safeguarding and child protection
Behaviour
Privacy notices
Anti bullying
Acceptable use agreement